



SEALED

Office of the United States Attorney  
District of Nevada  
501 Las Vegas Boulevard, Suite 1100  
Las Vegas, Nevada 89101  
(702) 388-6336

FILED

STEVEN W. MYHRE  
Acting United States Attorney  
District of Nevada  
CRISTINA D. SILVA  
PATRICK BURNS  
Assistant United States Attorneys  
501 Las Vegas Blvd. South, Ste. 1100  
Las Vegas, Nevada 89101  
Telephone: (702) 388-6336  
Fax (702) 388-6698  
[john.p.burns@usdoj.gov](mailto:john.p.burns@usdoj.gov)

2017 OCT 10 AM 9:36

U.S. MAGISTRATE JUDGE

BY \_\_\_\_\_

Attorney for the United States of America

**UNITED STATES DISTRICT COURT  
DISTRICT OF NEVADA**

-oOo-

IN THE MATTER OF THE SEARCH OF  
INFORMATION ASSOCIATED WITH  
EMAIL ACCOUNT  
CENTRALPARK4804@GMAIL.COM  
THAT IS STORED AT A PREMISES  
CONTROLLED BY GOOGLE.

Magistrate No. 17-mj-970-NJK

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH  
WARRANT**

(Under Seal)

STATE OF NEVADA     )  
                                  ) ss:  
COUNTY OF CLARK    )

**AFFIDAVIT IN SUPPORT OF AN  
APPLICATION FOR A SEARCH WARRANT**

I, Ryan S. Burke, Special Agent, Federal Bureau of Investigation (FBI), having  
been duly sworn, hereby depose and say:

**INTRODUCTION AND AGENT BACKGROUND**

1. Your Affiant makes this affidavit in support of an application for a search  
warrant for information associated with email account centralpark4804@gmail.com  
("Target Account"), an account associated with STEPHEN PADDOCK, that is stored at

1 a premises owned, maintained, controlled, or operated by Google, Inc. ("Google"), an  
2 American multinational technology based in Mountain View, California that specializes  
3 in Internet-related services and products. Those services include, but are not limited to,  
4 online advertising technologies, a search engine, email services, cloud computing, and  
5 many other services. The information to be searched is described in the following  
6 paragraphs and in Attachment "A" (attached hereto and incorporated herein by  
7 reference). This affidavit is made in support of an application for a search warrant under  
8 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require Google to disclose to the  
9 government records and other information in its possession, pertaining to the subscriber  
10 or customer associated with the Target Account.

11 2. I am an "investigative or law enforcement officer of the United States"  
12 within the meaning of Title 18, United States Code, Section 2510(7), that is, an officer of  
13 the United States who is empowered by law to conduct investigations of, and to make  
14 arrests for, offenses enumerated in Title 18, United States Code, Section 2516.

15 3. I have been employed as a Special Agent of the FBI for approximately five  
16 years, which began at the FBI Academy in October 2012. Upon completion of the  
17 academy, I was transferred to the Las Vegas Division's white collar crime squad and  
18 then the human trafficking squad. Since October 2015, I have been assigned to the Las  
19 Vegas Division's violent crime/gang squad. Additionally, I have been a certified member  
20 of the FBI's Cellular Analysis Survey Team since August 2015 due to my expertise in  
21 the field of historical cell site analysis.

22 4. During my tenure with the FBI, I have conducted surveillance, analyzed  
23 telephone records, interviewed witnesses, supervised activities of sources, executed  
24

1 search warrants, executed arrest warrants, and participated in court-authorized  
2 interceptions of wire and electronic communications. These investigative activities have  
3 been conducted in conjunction with a variety of investigations, to include those involving  
4 robbery, drug trafficking, kidnapping, murder, criminal enterprises, and more. In  
5 addition to my practical experiences, I received five months of extensive law enforcement  
6 training at the FBI Academy.

7 5. The facts in this affidavit are derived from your Affiant's personal  
8 observations, his training and experience, and information obtained from other agents,  
9 detectives, and witnesses. This affidavit is intended to show merely that there is  
10 sufficient probable cause for the requested warrant and does not set forth all of the  
11 Affiant's knowledge about this matter.

12 6. Based on your Affiant's training and experience and the facts as set forth  
13 in this affidavit, there is probable cause to believe that violations of:

- 14 a. Destruction/Damage of Aircraft or Aircraft Facilities - 18 U.S.C.A. § 32(a);  
15 b. Violence at International Airport - 18 U.S.C. § 37(a)(2); and  
16 c. Unlawful Interstate Transport/Delivery of Firearms by Non Federal  
17 Firearms Licensee – 18 USC 922(a)(3) and (5).

18 (hereafter, "Subject Offenses") have been committed by STEPHEN PADDOCK and  
19 others yet unknown. There is also probable cause to search the information described in  
20 Attachment "A" for evidence of these crimes and information which might reveal the  
21 identities of others involved in these crimes, as described in Attachment "B" (attached  
22 hereto and incorporated herein by reference).

23 ///

**PROBABLE CAUSE**

7. On the evening of Sunday, October 1, 2017, Route 91 Harvest, a music festival, was in progress at 3901 South Las Vegas Boulevard, Las Vegas, Nevada. At approximately 10:08 p.m., the Las Vegas Metropolitan Police Department (LVMPD) received calls reporting shots had been fired at the concert and multiple victims were struck. LVMPD determined the shots were coming from Rooms 134 and 135 on the 32nd floor of the Mandalay Bay Resort and Casino, located due west of the festival grounds at 3950 South Las Vegas Boulevard, Las Vegas, Nevada. These rooms are an elevated position which overlooks the concert venue. Witness statements and video footage captured during the attack indicates that the weapons being used were firing in a fully-automatic fashion.

8. LVMPD officers ultimately made entry into the room and located an individual later identified as Stephen Paddock. Paddock was deceased from an apparent self-inflicted gunshot wound.

9. Paddock's Nevada driver's license was located in the Mandalay Bay hotel room with Paddock, and both hotel rooms were registered in his name. A player's club card in name of Marilou Danley was located in Paddock's room, and the card returned to the address located on Babbling Brook Street in Mesquite, Nevada. FBI Agents located Danley, who was traveling outside the United States at the time of the shooting. It was ultimately determined that Danley resided with Paddock at the Babbling Brook address.

10. On October 2, 2017, search warrants were executed on Paddock's Mandalay Bay hotel rooms, Paddock's vehicle at Mandalay Bay, and two Nevada residences owed

1 by Paddock: 1372 Babbling Brook Court in Mesquite, and 1735 Del Webb Parkway in  
2 Reno, Nevada. Officers and Agents found over 20 firearms, hundreds of rounds of  
3 ammunition, and hundreds of spent shell casings in the Mandalay Bay hotel rooms, in  
4 close proximity to Paddock's body. Over a thousand rounds of rifle ammunition and 100  
5 pounds of explosive material was found in Paddock's vehicle. Additional explosive  
6 material, approximately 18 firearms, and over 1,000 rounds of ammunition was located  
7 at the Mesquite residence. A large quantity of ammunition and multiple firearms were  
8 recovered from the Reno residence.

9 11. As of this date, 58 people have been identified to have been killed in  
10 Paddock's attack and another 557 were reportedly injured. Additionally, investigators  
11 discovered that STEPHEN PADDOCK also utilized a firearm to shoot large fuel tanks  
12 on Las Vegas McCarran International Airport property. Multiple bullet holes were found  
13 on the tank, which investigators believe was an attempt by STEPHEN PADDOCK to  
14 cause the tanks to explode.

15 12. In an effort to determine whether or not STEPHEN PADDOCK was  
16 assisted and/or conspired with unknown individuals, investigators have attempted to  
17 identify all of STEPHEN PADDOCK's communication facilities. Based on a review of his  
18 financial accounts, email address centralpark1@live.com ("Account 2") was determined  
19 to belong to STEPHEN PADDOCK. On October 3, 2017, investigators requested an  
20 emergency disclosure of records from Microsoft related to Account 2 so it could be  
21 searched for any evidence of additional co-conspirators. Within the account,  
22 investigators identified the Target Account as one that required further investigation.

1           13.    On July 6, 2017, the Target Account sent an email to Account 2 that read,  
2    “try an ar before u buy. we have huge selection. located in the las vegas area.” Later that  
3    day, Account 2 sent an email to the Target Account that read, “we have a wide variety  
4    of optics and ammunition to try.” And lastly, Account 2 later sent an email to the Target  
5    Account that read, “for a thrill try out bumpfire ar’s with a 100 round magazine.”

6           14.    Based on the similarity of both email account names, investigators believe  
7    the Target Account may also be controlled by STEPHEN PADDOCK. Additionally,  
8    STEPHEN PADDOCK was previously a manager of an apartment complex in the Reno,  
9    Nevada area called “Central Park,” which investigators believe further substantiates his  
10   association to the Target Account. However, investigators have been unable to figure out  
11   why STEPHEN PADDOCK would be exchanging messages related to weapons that were  
12   utilized in the attack between two of his email accounts. Conversely, if the Target  
13   Account was not controlled by STEPHEN PADDOCK, investigators need to determine  
14   who was communicating with him about weapons that were used in the attack. Paddock  
15   acquired a substantial amount of firearms from out of state which appear to have been  
16   transported into the state of Nevada where he resides.

17          15.    Your Affiant believes the requested search warrant will yield significant  
18   information from Google such as STEPHEN PADDOCK’s contact list, email message  
19   content, IP address usage, photographs, third-party applications associated with the  
20   account, and more, which may constitute evidence of his planning of the attack and  
21   potentially identify other participants in the attack. Ultimately, your Affiant strongly  
22   believes the requested information will lead investigators to determine the full scope of  
23   STEPHEN PADDOCK’s plan.

**RELEVANT TECHNICAL TERMS**

16. The following non-exhaustive list of definitions applies to this Affidavit and the Attachments to this Affidavit:

a. The "Internet" is a worldwide network of computer systems operated by governmental entities, corporations, and universities. In order to access the Internet, an individual computer user must subscribe to an access provider, which operates a host computer system with direct access to the Internet. The World Wide Web is a functionality of the Internet which allows users of the Internet to share information.

b. "Internet Service Providers" are companies that provide access to the Internet. ISPs can also provide other services for their customers including website hosting, email service, remote storage, and co-location of computers and other communications equipment. ISPs offer different ways to access the Internet including telephone-based (dial-up), broadband-based access via a digital subscriber line (DSL) or cable television, dedicated circuits, or satellite-based subscription. ISPs typically charge a fee based upon the type of connection and volume of data (bandwidth). Many ISPs assign each subscriber an account name, such as a user name, an email address, and an email mailbox, and the subscriber typically creates a password for his/her account.

c. "ISP Records" are records maintained by ISPs pertaining to their subscribers (regardless of whether those subscribers are individuals or entities). These records may include account application information, subscriber and billing information, account access information (often in the form of log files), emails, information concerning content uploaded and/or stored on the ISP's servers, and other information, which may be stored both in computer data format and in written or printed record format. ISPs



1 reserve and/or maintain computer disk storage space on their computer system for their  
2 subscribers' use. This service by ISPs allows for both temporary and long-term storage  
3 of electronic communications and many other types of electronic data and files.

4 d. "Online service providers" (also referred to here as "service  
5 providers") are companies that provide online services such as email, chat or instant  
6 messaging, word processing applications, spreadsheet applications, presentation  
7 applications similar to PowerPoint, online calendar, photo storage and remote storage  
8 services. Sometimes they also can provide web hosting, remote storage, and co-location  
9 of computers and other communications equipment. Typically, each service provider  
10 assigns each subscriber an account name, such as a user name or screen name and the  
11 subscriber typically creates a password for his/her account.

12 e. "Computer," as used herein, is defined as "an electronic, magnetic,  
13 optical, electrochemical, or other high speed data processing device performing logical or  
14 storage functions, and includes any data storage facility or communications facility  
15 directly related to or operating in conjunction with such device."

16 f. A "server" is a centralized computer that provides services for other  
17 computers connected to it via a network. The other computers attached to a server are  
18 sometimes called "clients." For example, in a large company, it is common for individual  
19 employees to have client computers at their desktops. When the employees access their  
20 email, or access files stored on the network itself, those files are pulled electronically  
21 from the server, where they are stored, and are sent to the client's computer via the  
22 network. Notably, servers can be physically stored in any location: it is not uncommon  
23  
24

1 for a network's server to be located hundreds (and even thousands) of miles away from  
2 the client computers.

3 g. "Internet Protocol address," or "IP address," refers to a unique  
4 number used by a computer to access the Internet. IP addresses can be dynamic,  
5 meaning that the Internet Service Provider (ISP) assigns a different unique number to  
6 a computer every time it accesses the Internet. IP addresses might also be static, that  
7 is, an ISP assigns a user's computer a particular IP address which is used each time the  
8 computer accesses the Internet.

9 h. The term "domain" refers to a word used as a name for computers,  
10 networks, services, etc. A domain name typically represents a website, a server computer  
11 that hosts that website, or even some computer (or other digital device) connected to the  
12 internet. Essentially, when a website (or a server computer that hosts that website) is  
13 connected to the internet, it is assigned an IP address. Because IP addresses are difficult  
14 for people to remember, domain names are instead used because they are easier to  
15 remember than IP addresses. Domain names are formed by the rules and procedures of  
16 the Domain Name System (DNS). A common top level domain under these rules is ".com"  
17 for commercial organizations, ".gov" for the United States government, and ".org" for  
18 organizations. For example, www.usdoj.gov is the domain name that identifies a server  
19 used by the U.S. Department of Justice, and which uses IP address of 149.101.46.71.

20 i. "Web hosting services" maintain server computers connected to the  
21 Internet. Their customers use those computers to operate websites on the Internet.  
22 Customers of web hosting companies place files, software code, databases, and other data  
23  
24

1 on servers. To do this, customers typically connect from their own computers to the  
2 server computers across the Internet.

3 j. The term "WhoIs" lookup refers to a search of a publicly available  
4 online database that lists information provided when a domain is registered or when an  
5 IP address is assigned.

6 k. The terms "communications," "records," "documents," "programs," or  
7 "materials" include all information recorded in any form, visual or aural, and by any  
8 means, whether in handmade form (including, but not limited to, writings, drawings,  
9 paintings), photographic form (including, but not limited to, pictures or videos), or  
10 electrical, electronic or magnetic form, as well as digital data files. These terms also  
11 include any applications (i.e. software programs). These terms expressly include, among  
12 other things, emails, instant messages, chat logs, correspondence attached as to emails  
13 (or drafts), calendar entries, buddy lists.

14 l. "Chat" is usually a real time electronic communication between two  
15 or more individuals. Unlike email, which is frequently sent, then read and responded to  
16 minutes, hours, or even days later, chats frequently involve an immediate conversation  
17 between individuals, similar to a face-to-face conversation. Nearly all chat programs are  
18 capable of saving the chat transcript, to enable users to preserve a record of the  
19 conversation. By default, some chat programs have this capability enabled, while others  
20 do not. Many popular web-based email providers, like Google and Google, provide chat  
21 functionality as part of the online services they provide to account holders.

22 ///

23 ///

24

**FACTS ABOUT EMAIL PROVIDERS**

17. In my training, my experience and this investigation, I have learned that Google (the Service Provider) is a company that provides free web-based Internet email access to the general public, and that stored electronic communications, including opened and unopened email for Google subscribers may be located on the computers of Google. I have also learned that Google Inc. provides various on-line service messaging services to the general public. Instant Messaging ("IM") is a form of real-time direct text-based communication between two or more people using shared clients. The text is conveyed via devices connected over a network such as the Internet. In addition to text, Google's software allows users with the most current updated versions to utilize its webcam service. This option enables users from distances all over the world to view others who have installed a webcam on their end. Thus, the Service Provider's servers will contain a wide variety of the subscriber's files, including emails, address books, contact or buddy lists, calendar data, pictures, chat logs, and other files.

18. To use these services, subscribers register for online accounts like the Target Account. During the registration process, service providers such as the ones here ask subscribers to provide basic personal information. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit card or bank account number). Based on my training and my experience, I know that subscribers may insert false information to conceal their identity; even if this proves to be the case, however, I know that this information often provide clues to their identity, location or illicit activities.

1           19. In general, when a subscriber receives an email, it is typically stored in the  
2 subscriber's "mail box" on that service provider's servers until the subscriber deletes the  
3 Email. If the subscriber does not delete the message, the message (and any attachments)  
4 can remain on that service provider's servers indefinitely.

5           20. Similarly, when the subscriber sends an email, it is initiated at the  
6 subscriber's computer, transferred via the Internet to the service provider's servers, and  
7 then transmitted to its end destination. That service provider often saves a copy of the  
8 email sent. Unless the sender of the email specifically deletes the Email from the  
9 provider's server, the email can remain on the system indefinitely.

10           21. A sent or received email typically includes the content of the message,  
11 source and destination addresses, the date and time at which the email was sent, and  
12 the size and length of the email. If an email user writes a draft message but does not  
13 send it, that message may also be saved by that service provider, but may not include all  
14 of these categories of data.

15           22. Just as a computer on a desk can be used to store a wide variety of files, so  
16 can online accounts, such as the accounts subject to this application. First, subscribers  
17 can store many types of files as attachments to emails in online accounts. Second,  
18 because service providers provide the services listed above (e.g. word processing,  
19 spreadsheets, pictures), subscribers who use these services usually store documents on  
20 servers maintained and/or owned by service providers. Thus, these online accounts often  
21 contain documents such as pictures, audio or video recordings, logs, spreadsheets,  
22 applications and other files.

23. Reviewing files stored in online accounts raises many of the same difficulties as with reviewing files stored on a local computer. For example, based on my training, my experience and this investigation, I know that subscribers of these online services can conceal their activities by altering files before they upload them to the online service. Subscribers can change file names to more innocuous sounding names (e.g. renaming "FraudRecords.doc" to "ChristmasList.doc"), they can change file extensions to make one kind of file appear like a different type of file (e.g. changing the spreadsheet "StolenCreditProfiles.xls" to "FamilyPhoto.jpg" to appear to be a picture file, where the file extension ".xls" denotes an Excel spreadsheet file and ".jpg" a JPEG format image file), or they can change the times and dates a file was last accessed or modified by changing a computer's system time/date and then uploading that file to the Online Accounts. Thus, to detect any files that the subscriber may have concealed, agents will need to review all of the files in the Target Account; they will, however, only seize the items that the Court authorizes to be seized. Similarly, subscribers can conceal their activities by encrypting files. Thus, these files may need to be decrypted to detect whether it constitutes an Item to be Seized.

24. I also believe that people engaged in crimes such as the one described herein often use online accounts because they give people engaged in these crimes a way to easily communicate with other co-conspirators. Moreover, online accounts are easily concealed from law enforcement. Unlike physical documents, electronic documents can be stored in a physical place far away, where they are less likely to be discovered.

25. Service providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the

1 date on which the account was created, the length of service, records of log-in (i.e.,  
2 session) times and durations, the types of service utilized, the status of the account  
3 (including whether the account is inactive or closed), the methods used to connect to the  
4 account (such as logging into the account via websites controlled by the Service  
5 Provider), and other log files that reflect usage of the account. In addition, service  
6 providers often have records of the Internet Protocol address ("IP address") used to  
7 register the account and the IP addresses associated with particular logins to the  
8 account. Because every device that connects to the Internet must use an IP address, IP  
9 address information can help to identify which computers or other devices were used to  
10 access the online account.

11       26. In some cases, subscribers will communicate directly with a service  
12 provider about issues relating to the account, such as technical problems, billing  
13 inquiries, or complaints from or about other users. Service providers typically retain  
14 records about such communications, including records of contacts between the user and  
15 the provider's support services, as well records of any actions taken by the provider or  
16 user as a result of the communications.

17       27. In my training and experience, evidence of who was using an online  
18 account may be found in address books, contact or buddy lists, emails in the account,  
19 and pictures and files, whether stored as attachments or in the suite of the service  
20 provider's online applications. Therefore, the computers of the Service Providers are  
21 likely to contain stored electronic communications (including retrieved and un-retrieved  
22 email for their subscribers) and information concerning subscribers and their use of the  
23  
24

1 provider's services, such as account access information, email transaction information,  
2 documents, pictures, and account application information.

3 **INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**

4 28. Your Affiant anticipates executing this warrant under the Electronic  
5 Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and  
6 2703(c)(1)(A), by using the warrant to require Google to disclose to the government copies  
7 of the records and other information (including the content of communications)  
8 particularly described in Section I of Attachment "B." Upon receipt of the information  
9 described in Section I of Attachment "B," government-authorized persons will review  
10 that information to locate the items described in Section II of Attachment "B."

11 **CONCLUSION**

12 29. Based on the forgoing, I request that the Court issue the proposed search  
13 warrant. This Court has jurisdiction to issue the requested warrant because it is "a court  
14 of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A)  
15 & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has  
16 jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i). Pursuant to  
17 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the  
18 service or execution of this warrant.

19 **REQUEST FOR SEALING**

20 30. I further request that the Court order that all papers in support of this  
21 application, including the affidavit and search warrant, be sealed until further order of  
22 the Court. These documents discuss an ongoing criminal investigation that is neither  
23 public nor known to all of the targets of the investigation. Accordingly, there is good  
24



1 cause to seal these documents because their premature disclosure may seriously  
2 jeopardize that investigation.

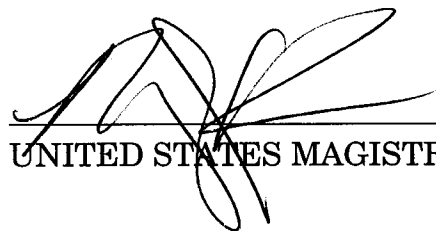
3  
4  
5 Respectfully Submitted,

6 

7 Ryan S. Burke, Special Agent  
8 Federal Bureau of Investigation

9 SWORN TO AND SUBSCRIBED

10 before me this 6<sup>th</sup> day of October 2017.

11 

12 UNITED STATES MAGISTRATE JUDGE  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24

**ATTACHMENT "A"**

**ONLINE ACCOUNT TO BE SEARCHED**

1. This warrant applies to information associated with the Google email account centralpark4804@gmail.com (the "Target Account") from its inception to present, which is stored at premises owned, maintained, controlled, or operated by Google, Inc., headquartered at 1600 Amphitheatre Way, Mountain View, California, 94043.

**ATTACHMENT "B"**  
**Particular Things to be Seized**

**I. Information to be disclosed by the Service Provider**

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, including any Emails, records, files, logs, or information that have been deleted but are still available to Service Provider, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Service Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A from account inception to present:

- a. The contents of all emails associated with the account, including copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. All records or other information stored in the Online Accounts, including address books, contact and buddy lists, calendar data, pictures, applications, documents, and other files;
- d. All records pertaining to communications between Service Provider and any person regarding the account, including contacts with support services and records of actions taken.
- e. All third-party application data and content associated with the Target Account through any Android operating system and/or any Google-related facility.

## ATTACHMENT "C"

**PROTOCOL FOR SEARCHING THE ELECTRONIC DATA SEIZED  
PURSUANT TO THIS SEARCH WARRANT**

1. In executing this warrant, the government must make reasonable efforts to use methods and procedures that will locate and expose in the electronic data produced in response to this search warrant ("the Search Warrant Data") those categories of data, files, documents, or other electronically stored information that are identified with particularity in the warrant, while minimizing exposure or examination of irrelevant, privileged, or confidential files to the extent reasonably practicable.

2. When the Search Warrant Data is received, the government will make a duplicate copy of the Search Warrant Data ("the Search Warrant Data Copy"). The original version of the Search Warrant Data will be sealed and preserved for purposes of: later judicial review or order to return or dispose of the Search Warrant Data; production to the defense in any criminal case if authorized by statute, rule, or the Constitution; for purposes of showing the chain of custody of the Search Warrant Data and the Search Warrant Data Copy; or for any other lawful purpose. The original of the Search Warrant Data will not be searched or examined except to ensure that it has been fully and completely replicated in the Search Warrant Data Copy.

3. The investigating agents will then search the entirety of the Search Warrant Data Copy using any and all methods and procedures deemed appropriate by the United States designed to identify the information listed as Information to be Seized in Attachment B, Section II. The United States may copy, extract or otherwise segregate information or data listed as Information to be Seized in Attachment B, Section II. Information or data so copied, extracted or otherwise segregated will no longer be subject to any handling restrictions that might be set out in this protocol beyond those required by binding law. To the extent evidence of crimes not within the scope of this warrant appear in plain view during this review, a supplemental or "piggyback" warrant will be applied for in order to further search that document, data, or other item.

4. Once the Search Warrant Data Copy has been thoroughly and completely examined for any document, data, or other items identified in Attachment B, Section II as Information to be Seized, the Search Warrant Data Copy will be sealed and not subject to any further search or examination unless authorized by another search warrant or other appropriate court order. The Search Warrant Data Copy will be held and preserved for the same purposes identified above in Paragraph 2.

1           5.       The search procedures utilized for this review are at the sole discretion of  
2 the investigating and prosecuting authorities, and may include the following techniques  
(the following is a non-exclusive list, as other search procedures may be used):

3           a.       examination of all of the data contained in the Search Warrant Data to view  
4 the data and determine whether that data falls within the items to be seized as set forth  
herein;

5           b.       searching for and attempting to recover from the Search Warrant Data any  
6 deleted, hidden, or encrypted data to determine whether that data falls within the list  
7 of items to be seized as set forth herein (any data that is encrypted and unreadable will  
not be returned unless law enforcement personnel have determined that the data is not  
(1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband,  
8 (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

9           c.       surveying various file directories and the individual files they contain;

10          d.       opening files in order to determine their contents;

11          e.       using hash values to narrow the scope of what may be found. Hash values  
are under- inclusive, but are still a helpful tool;

12          f.       scanning storage areas;

13          g.       performing keyword searches through all electronic storage areas to  
14 determine whether occurrences of language contained in such storage areas exist that  
are likely to appear in the evidence described in Attachment A; and/or

15          h.       performing any other data analysis technique that may be necessary to  
16 locate and retrieve the evidence described in Attachment B, Section II.

### 17       **Return and Review Procedures**

18          6.       Rule 41 of the Federal Rules of Criminal Procedure provides, in relevant  
part:

19               (e) Issuing the Warrant.

20               (2) Contents of the Warrant.

21               (A) Warrant to Search for and Seize a Person or Property. Except for a tracking-  
22 device warrant, the warrant must identify the person or property to be searched, identify  
any person or property to be seized, and designate the magistrate judge to whom it must  
23 be returned. The warrant must command the officer to:

1 (i) execute the warrant within a specified time no longer than 14 days;

2 (B) Warrant Seeking Electronically Stored Information. A warrant under Rule  
3 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or  
4 copying of electronically stored information. Unless otherwise specified, the warrant  
5 authorizes a later review of the media or information consistent with the warrant. The  
6 time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or  
7 on-site copying of the media or information, and not to any later off-site copying or  
8 review.

6 (f) Executing and Returning the Warrant.

7 (1) Warrant to Search for and Seize a Person or Property.

8 (B) Inventory. An officer present during the execution of the warrant must prepare  
9 and verify an inventory of any property seized. . . . In a case involving the seizure of  
10 electronic storage media or the seizure or copying of electronically stored information,  
11 the inventory may be limited to describing the physical storage media that were seized  
12 or copied. The officer may retain a copy of the electronically stored information that was  
13 seized or copied.

12 7. Pursuant to this Rule, the government understands and will act in  
13 accordance with the following:

14 a. Pursuant to Rule 41(e)(2)(A)(iii), within fourteen (14) days of the execution  
15 of the warrant, an agent is required to file an inventory return with the Court, that is,  
16 to file an itemized list of the property seized. Execution of the warrant begins when  
17 the United States serves the warrant on the named custodian; execution is complete  
18 when the custodian provides all Search Warrant Data to the United States. Within  
19 fourteen (14) days of completion of the execution of the warrant, the inventory will be  
20 filed.

18 b. Pursuant to Rule 41(e)(2)(B), Rule 41(e)(2)(A) governs the time within  
19 which the electronically stored information must be seized after the issuance of the  
20 warrant and copied after the execution of the warrant, not the "later review of the media  
21 or information" seized, or the later off-site digital copying of that media.

21 c. Under Rule 41(f)(1)(B), the inventory return that is to be filed with the court  
22 may be limited to a description of the "physical storage media" into which the Search  
23 Warrant Data that was seized was placed, not an itemization of the information or data  
24 stored on the "physical storage media" into which the Search Warrant Data was placed;

1 d. Under Rule 41(f)(1)(B), the government may retain a copy of that information for  
2 purposes of the investigation. The government proposes that the original storage media  
3 on which the Search Warrant Data was placed plus a full image copy of the seized Search  
Warrant Data be retained by the government.

4 e. If the person from whom any Search Warrant Data was seized requests the return  
5 of any information in the Search Warrant Data that is not set forth in Attachment B,  
6 Section II, that information will be copied onto appropriate media and returned to the  
7 person from whom the information was seized.  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24



SEALED

**Office of the United States Attorney**  
District of Nevada  
501 Las Vegas Boulevard, Suite 1100  
Las Vegas, Nevada 89101  
(702) 388-6336



FILED

STEVEN W. MYHRE  
Acting United States Attorney  
District of Nevada  
CRISTINA D. SILVA  
PATRICK BURNS  
Assistant United States Attorneys  
501 Las Vegas Blvd. South, Ste. 1100  
Las Vegas, Nevada 89101  
Telephone: (702) 388-6336  
Fax (702) 388-6698  
[john.p.burns@usdoj.gov](mailto:john.p.burns@usdoj.gov)

2017 OCT 10 AM 9:36

U.S. MAGISTRATE JUDGE

BY \_\_\_\_\_

Attorney for the United States of America

UNITED STATES DISTRICT COURT  
DISTRICT OF NEVADA

-oOo-

IN THE MATTER OF THE SEARCH OF  
INFORMATION ASSOCIATED WITH  
EMAIL ACCOUNT  
CENTRALPARK4804@GMAIL.COM  
THAT IS STORED AT A PREMISES  
CONTROLLED BY GOOGLE.

Magistrate No. 17-mj-970-NJK

(Under Seal)

**GOVERNMENT'S APPLICATION REQUESTING  
SEALING OF AFFIDAVIT**

COMES NOW the United States of America, by and through STEVEN W.  
MYHRE, Acting United States Attorney, and PATRICK BURNS, Assistant United States  
Attorney, and respectfully moves this Honorable Court for an Order sealing the Affidavit,  
together with the Court's Order, in the above-captioned matter until such time as this Honorable  
Court, or another Court of competent jurisdiction, shall order otherwise.

The Government submits that it is necessary for said documents to be sealed in light of  
the fact that they make reference to information regarding an on-going investigation.

///

1 The Government submits that disclosure of the information might possibly jeopardize the  
2 investigation. The Government submits that its right to secrecy far outweighs the public's right  
3 to know.

4 DATED this 6 day of October 2017.  
5

6  
7 Respectfully submitted,  
8 STEVEN W. MYHRE  
9 Acting United States Attorney

10 *KMacfadden FOR*  
11 PATRICK BURNS  
12 Assistant United States Attorney  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26

UNITED STATES DISTRICT COURT

DISTRICT OF NEVADA

-oOo-

I IN THE MATTER OF THE SEARCH OF  
INFORMATION ASSOCIATED WITH  
EMAIL ACCOUNT  
CENTRALPARK4804@GMAIL.COM THAT  
IS STORED AT A PREMISES  
CONTROLLED BY GOOGLE.

Magistrate No. 17-mj-970-NJK

(Under Seal)

SEALING ORDER

Based on the pending Application of the Government, and good cause appearing therefor,

IT IS HEREBY ORDERED that the Affidavit, together with the Court's Order, in  
the above-captioned matter shall be sealed until further Order of the Court.

DATED this 6th day of October, 2017.

  
UNITED STATES MAGISTRATE JUDGE

AO 93 (Rev. 11/13) Search and Seizure Warrant

FILED

## UNITED STATES DISTRICT COURT

for the  
District of Nevada

2017 OCT 10 AM 9:36

U.S. MAGISTRATE JUDGE

BY \_\_\_\_\_

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)

EMAIL ACCOUNT CENTRALPARK4804@GMAIL.COM

Case No. 2:17-mj- 970-NJK

## SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the \_\_\_\_\_ District of \_\_\_\_\_ Nevada  
(identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

SEE ATTACHMENTS B and C

**YOU ARE COMMANDED** to execute this warrant on or before October 20, 2017 (not to exceed 14 days)  
☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Nancy J. Koppe

(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)☐ for \_\_\_\_\_ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of \_\_\_\_\_Date and time issued: 10/10/2017 8:30 pmCity and state: Las Vegas, Nevada

Judge's signature

Printed name and title

Nancy J. Koppe, US Magistrate Judge

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

**Return**

Case No.:

2:17-mj-

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

**Certification**

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: \_\_\_\_\_

\_\_\_\_\_  
*Executing officer's signature*\_\_\_\_\_  
*Printed name and title*



SEALED

Office of the United States Attorney  
District of Nevada  
501 Las Vegas Boulevard, Suite 1100  
Las Vegas, Nevada 89101  
(702) 388-6336

**ATTACHMENT "A"**

**ONLINE ACCOUNT TO BE SEARCHED**

1. This warrant applies to information associated with the Google email account centralpark4804@gmail.com (the "Target Account") from its inception to present, which is stored at premises owned, maintained, controlled, or operated by Google, Inc., headquartered at 1600 Amphitheatre Way, Mountain View, California, 94043.

**ATTACHMENT "B"**  
**Particular Things to be Seized**

**I. Information to be disclosed by the Service Provider**

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, including any Emails, records, files, logs, or information that have been deleted but are still available to Service Provider, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Service Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A from account inception to present:

- a. The contents of all emails associated with the account, including copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. All records or other information stored in the Online Accounts, including address books, contact and buddy lists, calendar data, pictures, applications, documents, and other files;
- d. All records pertaining to communications between Service Provider and any person regarding the account, including contacts with support services and records of actions taken.
- e. All third-party application data and content associated with the Target Account through any Android operating system and/or any Google-related facility.



## II. Information to be seized by the United States

After reviewing all information described in Section I, the United States will seize evidence of violations of Title 18, United States Code Sections 32(a) (Destruction/Damage of Aircraft or Aircraft Facilities); 37(a)(2) (Violence at International Airport); and 922(a)(3); 5 (Unlawful Interstate Transport/Delivery of Firearms by Non Federal Firearms Licensee) (the "Subject Offenses") that occur in the form of the following, from account inception to present:

- a. Communications, transactions and records that may establish ownership and control (or the degree thereof) of the Target Account, including address books, contact or buddy lists, bills, invoices, receipts, registration records, bills, correspondence, notes, records, memoranda, telephone/address books, photographs, video recordings, audio recordings, lists of names, records of payment for access to newsgroups or other online subscription services, and attachments to said communications, transactions and records.
- b. Communications, transactions and records to/from persons who may be co-conspirators of the Subject Offenses, or which may identify co-conspirators.
- c. Communications, transactions and records which may show motivation to commit the Subject Offenses.
- d. Communications, transactions and records that relate to the Subject Offenses.
- e. The terms "communications," "transactions," "records," "documents," "programs," or "materials" include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, paintings), photographic form (including, but not limited to, pictures or videos), or electrical, electronic or magnetic form, as well as digital data files. These terms also include any applications (i.e. software programs). These terms expressly include, among other things, Emails, instant messages, chat logs, correspondence attached as to Emails (or drafts), calendar entries, buddy lists.

## ATTACHMENT "C"

**PROTOCOL FOR SEARCHING THE ELECTRONIC DATA SEIZED  
PURSUANT TO THIS SEARCH WARRANT**

1. In executing this warrant, the government must make reasonable efforts to use methods and procedures that will locate and expose in the electronic data produced in response to this search warrant ("the Search Warrant Data") those categories of data, files, documents, or other electronically stored information that are identified with particularity in the warrant, while minimizing exposure or examination of irrelevant, privileged, or confidential files to the extent reasonably practicable.

2. When the Search Warrant Data is received, the government will make a duplicate copy of the Search Warrant Data ("the Search Warrant Data Copy"). The original version of the Search Warrant Data will be sealed and preserved for purposes of: later judicial review or order to return or dispose of the Search Warrant Data; production to the defense in any criminal case if authorized by statute, rule, or the Constitution; for purposes of showing the chain of custody of the Search Warrant Data and the Search Warrant Data Copy; or for any other lawful purpose. The original of the Search Warrant Data will not be searched or examined except to ensure that it has been fully and completely replicated in the Search Warrant Data Copy.

3. The investigating agents will then search the entirety of the Search Warrant Data Copy using any and all methods and procedures deemed appropriate by the United States designed to identify the information listed as Information to be Seized in Attachment B, Section II. The United States may copy, extract or otherwise segregate information or data listed as Information to be Seized in Attachment B, Section II. Information or data so copied, extracted or otherwise segregated will no longer be subject to any handling restrictions that might be set out in this protocol beyond those required by binding law. To the extent evidence of crimes not within the scope of this warrant appear in plain view during this review, a supplemental or "piggyback" warrant will be applied for in order to further search that document, data, or other item.

4. Once the Search Warrant Data Copy has been thoroughly and completely examined for any document, data, or other items identified in Attachment B, Section II as Information to be Seized, the Search Warrant Data Copy will be sealed and not subject to any further search or examination unless authorized by another search warrant or other appropriate court order. The Search Warrant Data Copy will be held and preserved for the same purposes identified above in Paragraph 2.

5. The search procedures utilized for this review are at the sole discretion of the investigating and prosecuting authorities, and may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

a. examination of all of the data contained in the Search Warrant Data to view the data and determine whether that data falls within the items to be seized as set forth herein;

b. searching for and attempting to recover from the Search Warrant Data any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

c. surveying various file directories and the individual files they contain;

d. opening files in order to determine their contents;

e. using hash values to narrow the scope of what may be found. Hash values are under-inclusive, but are still a helpful tool;

f. scanning storage areas;

g. performing keyword searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment A; and/or

h. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B, Section II.

### **Return and Review Procedures**

6. Rule 41 of the Federal Rules of Criminal Procedure provides, in relevant part:

(e) Issuing the Warrant.

(2) Contents of the Warrant.

(A) Warrant to Search for and Seize a Person or Property. Except for a tracking-device warrant, the warrant must identify the person or property to be searched, identify any person or property to be seized, and designate the magistrate judge to whom it must be returned. The warrant must command the officer to:

1 (i) execute the warrant within a specified time no longer than 14 days;

2 (B) Warrant Seeking Electronically Stored Information. A warrant under Rule  
3 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or  
4 copying of electronically stored information. Unless otherwise specified, the warrant  
5 authorizes a later review of the media or information consistent with the warrant. The  
6 time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or  
7 on-site copying of the media or information, and not to any later off-site copying or  
8 review.

6 (f) Executing and Returning the Warrant.

7 (1) Warrant to Search for and Seize a Person or Property.

8 (B) Inventory. An officer present during the execution of the warrant must prepare  
9 and verify an inventory of any property seized. . . . In a case involving the seizure of  
10 electronic storage media or the seizure or copying of electronically stored information,  
11 the inventory may be limited to describing the physical storage media that were seized  
or copied. The officer may retain a copy of the electronically stored information that was  
seized or copied.

12 7. Pursuant to this Rule, the government understands and will act in  
13 accordance with the following:

14 a. Pursuant to Rule 41(e)(2)(A)(iii), within fourteen (14) days of the execution  
15 of the warrant, an agent is required to file an inventory return with the Court, that is,  
16 to file an itemized list of the property seized. Execution of the warrant begins when  
17 the United States serves the warrant on the named custodian; execution is complete  
when the custodian provides all Search Warrant Data to the United States. Within  
fourteen (14) days of completion of the execution of the warrant, the inventory will be  
filed.

18 b. Pursuant to Rule 41(e)(2)(B), Rule 41(e)(2)(A) governs the time within  
19 which the electronically stored information must be seized after the issuance of the  
20 warrant and copied after the execution of the warrant, not the "later review of the media  
or information" seized, or the later off-site digital copying of that media.

21 c. Under Rule 41(f)(1)(B), the inventory return that is to be filed with the court  
22 may be limited to a description of the "physical storage media" into which the Search  
23 Warrant Data that was seized was placed, not an itemization of the information or data  
24 stored on the "physical storage media" into which the Search Warrant Data was placed;

1 d. Under Rule 41(f)(1)(B), the government may retain a copy of that information for  
2 purposes of the investigation. The government proposes that the original storage media  
3 on which the Search Warrant Data was placed plus a full image copy of the seized Search  
Warrant Data be retained by the government.

4 e. If the person from whom any Search Warrant Data was seized requests the return  
5 of any information in the Search Warrant Data that is not set forth in Attachment B,  
6 Section II, that information will be copied onto appropriate media and returned to the  
7 person from whom the information was seized.  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24

## UNITED STATES DISTRICT COURT

for the

District of Nevada

In the Matter of the Search of )

(Briefly describe the property to be searched  
or identify the person by name and address) )

EMAIL ACCOUNT CENTRALPARK4804@GMAIL.COM )

Case No. 2:17-mj- 970-NJK

## SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the \_\_\_\_\_ District of \_\_\_\_\_ Nevada  
(identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

SEE ATTACHMENTS B and C

**YOU ARE COMMANDED** to execute this warrant on or before October 20, 2017 (not to exceed 14 days)  
☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Alex J. Koppe

(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for \_\_\_\_\_ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of \_\_\_\_\_

Date and time issued: 10/6/2017 8:30 pm

Judge's signature

City and state: Las Vegas, Nevada

Alex J. Koppe  
 Printed name and title  
 US Magistrate Judge

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

## Return

FILED

Case No.:

2:17-mj- 970-NJK

Date and time warrant executed:

10/6/17 @ 23:07

Copy of warrant and inventory left with:

N/A

2017 NOV 17 AM 10:40

Inventory made in the presence of:

N/A

U.S. MAGISTRATE JUDGE

Inventory of the property taken and name of any person(s) seized:

BY \_\_\_\_\_

Google provided 9 files regarding centralpark4804@gmail.com, totaling approximately 910 KB in size.

## Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: \_\_\_\_\_

\_\_\_\_\_  
Executing officer's signature\_\_\_\_\_  
Printed name and title